

FORM PTO-1449

Attorney Docket:
0225-4188Serial No.:
09/498,716

INFORMATION DISCLOSURE CITATION

Applicant:
Lenstra et al.Filing Date:
February 7, 2000Group Art Unit:
2766

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
<i>MH/4/03</i>	AA	5,787,028	07/28/98	Mullin			
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

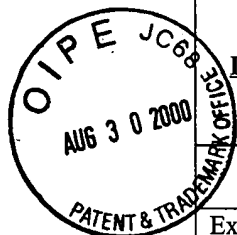
<i>MH/4/03</i>	AR	R.C. Mullin et al., "Optimal Normal Bases in GF(p)*", <u>Discrete Applied Mathematics</u> , 22 (1988/89), pp. 149-161.
	AS	
	AT	

Examiner

Date Considered

EXAMINER:

Initial if reference considered, whether or not citation is in conformance with MPEP §609.
 Draw line through citation if not in conformance and not considered.
 Include copy of this form with next communication to Applicant.



RECEIVED
 SEP - 1 2000
 TC 2700 MAIL ROOM



↑AFFIX CUSTOMER NO. LABEL ABOVE ↑

Page 1 of 1

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Attorney Docket:
0225-4188Serial No.:
09/498,716Applicant:
Lenstra et al.Filing Date:
February 7, 2000Group Art Unit:
2766

U.S. PATENT DOCUMENTS

Examiner Initial		Patent Number	Publication Date	Name	Class	Sub-Class	Filing Date
<i>n/h</i>	AA	6,252,960 B1	6/26/2001	Serroussi			
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

Examiner Initial		Patent Number	Publication Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Papers, etc.)

<i>n/h</i>	AR	Brouwer et al.; "Doing More with Fewer Bits"; Advances in Cryptology-Asiacrypt' 99, 1999, pgs. 321-332.
	AS	
	AT	

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.



FORM PTO-1449				Attorney Docket: 0225-4188	Serial No.: 09/498,716
INFORMATION DISCLOSURE CITATION				Applicant: Lenstra et al.	Group Art Unit: 2766
				Filing Date: 02/07/00	
U.S. PATENT DOCUMENTS					
Examiner Initial		Document Number	Date	Name	Class Sub- Class
M/H 11/20/03	AA	4,587,627	05/06/86	Omura	
M/H 11/20/03	AB	5,406,628	04/11/95	Beller et al.	
M/H 11/20/03	AC	5,481,613	01/02/96	Ford et al.	
M/H 11/20/03	AD	4,745,568	05/17/88	Onyszchuk et al.	
M/H 11/20/03	AE	4,995,082	02/19/91	Schnorr	
M/H 11/20/03	AF	5,231,668	07/27/93	Kravitz	
M/H 11/20/03	AG	5,351,297	09/27/94	Miyaji et al.	
M/H 11/20/03	AH	5,442,707	08/15/95	Miyaji et al.	
M/H 11/20/03	AI	4,405,829	09/83	Rivest et al.	
M/H 11/20/03	AJ	4,870,681	09/89	Sedlak	
	AK				
FOREIGN PATENT DOCUMENTS					
		Document Number	Date	Country	Class Sub- Class
M/H 11/20/03	AL	WO 85/01625	04/11/85	WIPO	
	AM				
OTHER DOCUMENTS (Including Author, Title, Date, etc.)					
M/H 10/20/03	AR	Neal Koblitz, "A Course in Number Theory and Cryptography," Springer, pp. 87-89, 99-106, 178-182.			
M/H 11/20/03	AS	Bruce Schneier, "Applied Cryptography", 2e, John Wiley & Sons, Inc., pp. 496-499			
M/H 11/20/03	AT	P. Duhamel et al., "A Decomposition of the Arithmetic for NTT's with 2 as a Root of Unity," ICASSP '84.			
M/H 11/20/03	AU	R.L. Rivest et al., "A Method for Obtaining Digital Structures and Public-Key Cryptosystems", <i>Communications of the ACM</i> , Vol. 21, No. 2, pp. 120-126, 1978.			
M/H 11/20/03	AV	A.K. Lenstra and H.W. Lenstra Jr., "Algorithms in Number Theory", <i>Handbook of Theoretical Computer Science</i> , pp. 675-715, 1990.			
M/H 11/20/03	AW	D. Coppersmith, "Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known", <i>EUROCRYPT '96, Proceedings</i> , LNCS 1070, pp. 178-189, 1996.			
M/H 11/20/03	AX	S. Garfinkel, "PBP: Pretty Good Privacy," 1995, pp. 42-43.			
Examiner	M. H. 11/20/03			Date Considered	11/21/03
EXAMINER	Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.				

RECEIVED
AUG 28 2000
TC 2700 MAIL ROOM



FORM PTO-1449

INFORMATION DISCLOSURE CITATIONAttorney Docket:
0225-4188Serial No.:
09/498,716Applicant:
Lenstra et al.Filing Date:
02/07/00Group/Art Unit:
2766**U.S. PATENT DOCUMENTS**

Examiner Initial	Document Number	Date	Name	Class	Sub-Class	Filing Date
AA						
AB						
AC						
AD						
AE						
AF						
AG						
AH						
AI						
AJ						

FOREIGN PATENT DOCUMENTS

Document Number	Date	Country	Class	Sub-Class	Translation
AL					<input type="checkbox"/> Yes <input type="checkbox"/> No
AM					<input type="checkbox"/> Yes <input type="checkbox"/> No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

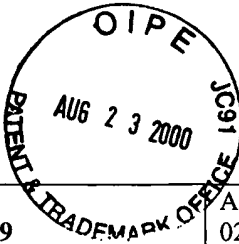
11/21/03	AR	Coppersmith and Andrew Odlyzko, "Discrete Logarithms in GF(p)", Algorithmica, Volume 1, No. 1, 1986; pp. 1-15.
11/21/03	AS	Guillou and Quisquater, "Precautions Taken against Various Potential Attacks", Eurocrypt '90, Springer 1990, pp. 465-473.
11/21/03	AT	"Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", ITU-T Recommendation X-509, ISO/IEC 9594-8: 1995(E), pp. 1-35. 1995.
11/21/03	AU	Agnew, G.B. et al., "An Implementation for a Fast Public-Key Cryptosystem", Journal of Cryptology, 1991, Vol. 3, pp. 63-79.
11/21/03	AV	Robert D. Silverman, "Fast Generation of Random, Strong RSA Primes", RSA Laboratories' CryptoBytes, Vol 3, No. 1, pp. 9-13, Spring 1997.
11/21/03	AW	Ohta et al., (Eds), "Advances in Cryptology", CRYPTO '98, pp. 1-10.
11/21/03	AX	Arjen K. Lenstra, "Generating RSA Moduli with a Predetermined Portion," Advances in Cryptology, ASIACRYPT '98, Beijing, China, Oct. 18-22, 1998; pp. 1-10.

Examiner

Date Considered

EXAMINER:

Initial if reference considered, whether or not citation is in conformance with MPEP §609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.



Page 2 of 2
RECEIVED
AUG 28 2000
IC 2100 MAIL ROOM

FORM PTO-1449		Attorney Docket: 0225-4188		Serial No.: 09/498,719		
INFORMATION DISCLOSURE CITATION		Applicant: Lenstra et al.		Group Art Unit: 2766		
		Filing Date: 02/07/00				
U.S. PATENT DOCUMENTS						
Examiner Initial		Document Number	Date	Name	Class Sub-Class	Filing Date
	AA					
	AB					
	AC					
	AD					
	AE					
	AF					
	AG					
	AH					
	AI					
	AJ					
	AK					
FOREIGN PATENT DOCUMENTS						
		Document Number	Date	Country	Class Sub-Class	Translation
	AL					<input type="checkbox"/> Yes <input type="checkbox"/> No
OTHER DOCUMENTS (Including Author, Title, Date, etc.)						
M/H 11/21/03	AR	Guillou, Davio and Quisquater, "Public Key Techniques: Randomness and Redundancy", Cryptologia, 1989, pp. 167-182.				
M/H 11/21/03	AS	S. Gao and H. Lenstra, "Optimal Normal Bases, Codes and Cryptography," 2, pp. 315-323.				
M/H 11/21/03	AT	Elwyn R. Berlekamp, "Algebraic Coding Theory" revised 1984 edition, Aegean Park Press, Chapter 10				
M/H 11/21/03	AU	U.M. Maurer, "Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters", <i>Journal of Cryptology</i> , Vol. 8, pg 123-155, 1995.				
M/H 11/21/03	AV	P.L. Montgomery, "Modular Multiplication Without Trial Division", <i>Mathematics of Computation</i> , Vol. 44, No. 170, pp. 519-521, 1985.				
M/H 11/21/03	AW	Vanstone et al., "Short RSA Keys and Their Generation", <i>Journal of Cryptology</i> , Spring 1995, vol. 8, no. 2, pp. 101-114.				
M/H 11/21/03	AX	Young, A. et al., "The dark side of "black-box" cryptography or: Should we trust Capstone", <i>Advances on Cryptology</i> , CRYPTO '96, Aug. 18-22, 1996; pp. 89-103.				
M/H 11/21/03	AY	Vanstone et al., "Using Four-Prime RSA in which some of the Bits are Specified," <i>Electronics Letters</i> , GV, IEE Stevenage, vol. 30, no. 25, 08/12/94, pp. 2118-2119.				
Examiner		M. H. H. H. C.		Date Considered 11/21/03		
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.						



#9

Page 1 of 1

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial	Patent Number	Publication Date	Name	Class	Sub-Class	Filing Date

FOREIGN PATENT DOCUMENTS

Examiner Initial	Patent Number	Publication Date	Country	Class	Sub-Class	Translation
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No
						<input type="checkbox"/> Yes <input type="checkbox"/> No

OTHER DOCUMENTS (continued)

M/H 1/2/03	Lenstra et al. "Fast Irreducibility and Subgroup Membership Testing in XTR", Public Key Cryptography, Kim (ed) Springer-Verlag, 2001
M/H 11/2/03	Lenstra et al. "The XTR Public Key System", (extended version of Crypto 2000 Presentation), pp. 73-86
M/H 11/2/03	"Chapter 12. A New Public-Key Cryptosystem" pp. 1-11
M/H 11/2/03	"The XTR Cryptosystem", Internet, Sept. 2001, pp. 1-5
M/H 11/2/03	More "Letter to DDJ", Doctor Dobb's Journal on CD-Rom, May 1993, pp. 2-3
M/H 11/2/03	Smith "Cryptography Without Exponentiation", Dr. Dobb's Journal on CD-Rom, Apr. 1994, pp. 1-3
M/H 11/2/03	Smith "LUC Public-Key Encryption", Dr. Dobb's Journal on CD-Rom, Jan. 1993, pp. 1-12
M/H 11/2/03	McEliece "Finite Fields for Computer Scientists and Engineers", Kluwer Academic Publishers, 1987, pp. 96-119
M/H 11/2/03	Gong et al. "Public-Key Cryptosystems Based on Cubic Finite Field Extensions", IEEE Transactions on Information Theory, Vol. 45, No. 7, Nov. 1999, pp. 2601-2605
M/H 11/2/03	Menezes et al. "Handbook of Applied Cryptography", CRC Press, 1997
M/H 11/2/03	Lenstra et al. "Key Improvements to XTR", Asiacrypt, 2000

Examiner <i>M. H. [Signature]</i>	Date Considered 11/20/03
EXAMINER Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.	

FORM PTO-1449 INFORMATION DISCLOSURE CITATION				Attorney Docket: 0225-4188		Serial No.: 09/498,716	
				Applicant: Lenstra et al.			
				Filing Date: 02/07/00		Group Art Unit: Unassigned	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No
OTHER DOCUMENTS (Including Author, Title, Date, etc.)							
<i>M/H 11/20/03</i>	AR	Bailey et al., "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms," Advances in Cryptology, Crypto '98, 18th Annual Int'l Cryptology Conference, August 23-27, pp. 473-485.					
<i>M/H 11/20/03</i>	AS	Brouwer et al., "Doing More with Few Bits," Advances in Cryptology: Proceedings/ASIACRYPT '99, Int'l Conference on the Theory Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, pp. 321-332.					
<i>M/H 11/20/03</i>	AT	Cohen et al., "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates," Advances in Cryptology: Proceedings/ASIACRYPT '98, Beijing, China, October 18-22, 1998, pp. 51-65.					
Examiner <i>M. H. H. L.</i>				Date Considered <i>11/20/03</i>			
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.							

FORM PTO-1449 INFORMATION DISCLOSURE CITATION				Attorney Docket: 0225-4188		Serial No.: 09/498,716	
				Applicant: Lenstra et al.			
				Filing Date: 02/07/00		Group Art Unit: Unassigned	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No
OTHER DOCUMENTS (Including Author, Title, Date, etc.)							
<i>M/H 11/2/03</i>	AR	Cramer et al. "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," Advances in Cryptology: Proceedings/Crypto '98, 18th Annual Int'l Cryptology Conference, Santa Barbara, Aug. 23-27, 1998; pp. 13-25.					
<i>M/H 11/2/03</i>	AS	Taher Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, July 1985, pp. 469-472.					
<i>M/H 11/29/03</i>	AT	P. Gaudry et al., "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," pp. 1-19.					
Examiner <i>M/H 11/2/03</i>				Date Considered <i>11/20/03</i>			
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.							

FORM PTO-1449 <u>INFORMATION DISCLOSURE CITATION</u>				Attorney Docket: 0225-4188		Serial No.: 09/498,716	
				Applicant: Lenstra et al.			
				Filing Date: 02/07/00		Group Art Unit: Unassigned	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No
OTHER DOCUMENTS (Including Author, Title, Date, etc.)							
<i>M/H 11/20/03</i>	AR	*4.3.3 "How Fast Can We Multiply", Arithmetic, Addison-Wesley Publishing Co., Inc., 1981, pp. 278-281.					
<i>M/H 11/24/03</i>	AS	Arjen K. Lenstra, "Using Cyclotomic Polynomials to Construct Efficient Discrete Logarithm Cryptosystems over Finite Fields," ACISP '97, Sydney, Australia, July 7-9, 1997, pp. 127-138.					
<i>M/H 11/20/03</i>	AT	Arjen K. Lenstra, "Generating RSA Moduli with a Predetermined Portion," ASIACRYPT '98, Beijing, Cinga, October 18-22, 1998, pp. 1-10.					
Examiner <i>M. T. L. H. C.</i>				Date Considered <i>11/20/03</i>			
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.							

FORM PTO-1449 INFORMATION DISCLOSURE CITATION				Attorney Docket: 0225-4188		Serial No.: 09/498,716	
				Applicant: Lenstra et al.			
				Filing Date: 02/07/00		Group Art Unit: Unassigned	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AM						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AN						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AO						<input type="checkbox"/> Yes <input type="checkbox"/> No
	AP						<input type="checkbox"/> Yes <input type="checkbox"/> No
OTHER DOCUMENTS (Including Author, Title, Date, etc.)							
11/2/03	AR	Alfred Menezes, "Comparing the Security of ECC and RSA", Alfred Menezes Home Page, supplement to article by B. Schneier, "Elliptic Curve Public-Key Cryptography, Nov. 1999; pp. 1-4.					
11/2/03	AS	C.P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, 1981; pp. 161-174.					
11/2/03	AT	P. Smith et al., "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," ASIACRYPT'94, November 28 - December 1, 1994; pp. 357-364.					
Examiner <i>M. H. L. H. L.</i>				Date Considered <i>11/20/03</i>			
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.							